白皮书
2019-07

IMT-2020
IMT-2020 (5G) 推进组

LTE-V2X 安全技术

目录

1 概述 P1

2 LTE-V2X车联网系统安全风险 P2

3 LTE-V2X车联网系统安全需求 P6

4 LTE-V2X车联网系统安全架构及机制 P8

5 总结与展望 P21

6 主要贡献单位 P22

IMT-2020(5G)推进组于2013年2月由中国工业和信息化部、国家发展和改革委员会、科学技术部联合推动成立，组织架构基于原IMT-Advanced推进组，成员包括中国主要的运营商、制造商、高校和研究机构。推进组是聚合中国产学研用力量、推动中国第五代移动通信技术研究和开展国际交流与合作的主要平台。

1 概述

C-V2X是基于蜂窝（Cellular）通信演进形成的车用无线通信技术（Vehicle to Everything，V2X）技术，可提供Uu接口（蜂窝通信接口）和PC5接口（直连通信接口）。

基于LTE网络的V2X通信技术作为C-V2X现阶段主要解决方案，引起了国内外政府、汽车、芯片、电子设备及网络设备、交通管理、电信运营、业务服务以及学术界等各行业的广泛关注，得到了全球运营商、汽车厂商的普遍支持。

LTE-V2X车联网系统的组成架构、通信场景对系统安全保障、用户隐私保护等方面提出了新的需求与挑战。本白皮书在安全风险分析的基础上，深入研究LTE-V2X车联网系统信息安全需求及机制，同时结合我国实际情况，试验性提出车联网安全基础设施部署方案，为我国LTE-V2X商用系统实际部署以及LTE-V2X车联网业务数据安全和用户隐私保护方案提供参考。

2 LTE-V2X车联网系统安全风险

LTE-V2X车联网系统包含云、管、端几大方面，系统架构如图2-1所示。本节从网络通信、业务应用、车载终端、路侧设备等方面论述LTE-V2X车联网系统面临的安全风险。

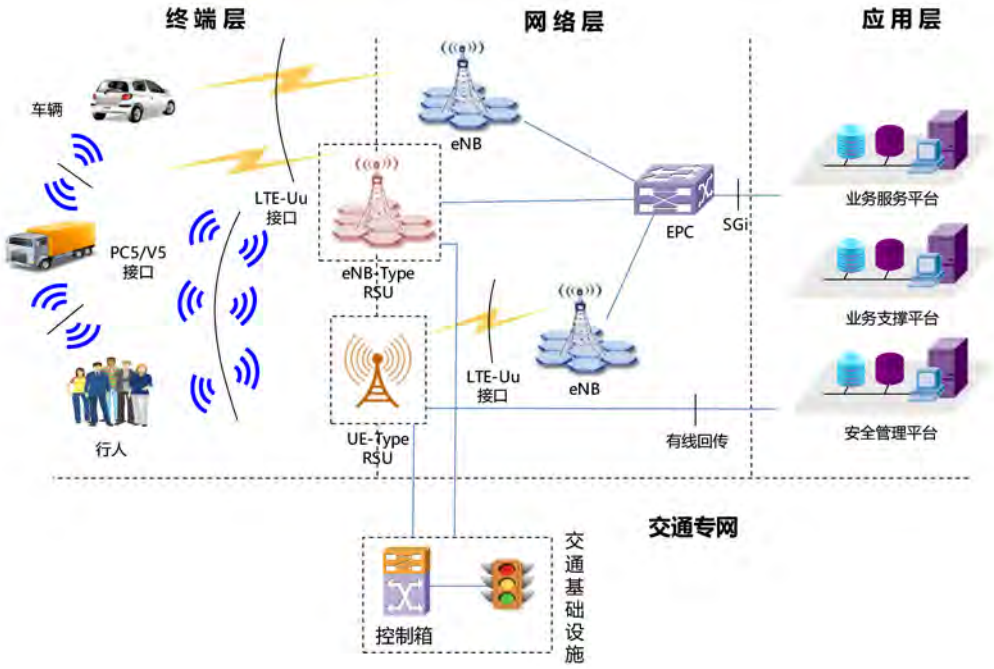


图2-1　LTE-V2X车联网系统示意图

2.1 网络通信

2.1.1　蜂窝通信接口

蜂窝通信接口场景下，LTE-V2X车联网系统继承了传统LTE网络系统面临的安全风险，主要有假冒终端、伪基站、信令/数据窃听、信令/数据篡改/重放等。

在未经保护的情况下，非法终端可以假冒合法终端的身份接入运营商的蜂窝网络，占用网络资源，获取网络服务。同时，假冒合法终端身份，发送伪造的网络信令或业务数据信息,影响系统的正常运行。

攻击者部署虚假的LTE网络基站并通过发射较强的无线信号吸引终端选择并接入，造成网络数据

连接中断，直接危害车联网业务安全。

利用LTE-Uu接口的开放性以及网络传输链路上的漏洞，攻击者可以窃听车联网终端与网络间未经保护直接传输的网络信令/业务数据，获取有价值的用户信息，例如短消息、车辆标识、状态、位置等，造成用户隐私泄露；攻击者可以发起中间人攻击，篡改车联网终端与网络间未保护直接传输的网络信令/业务数据，或者重新发送过期的网络信令/业务数据，导致网络服务中断或者业务数据错误，出现异常的行为及结果，危害LTE-V2X车联网业务安全。

2.1.2 直连通信接口

不论是基站集中式调度模式（Mode 3）还是终端分布式调度模式（Mode 4），直连传输的用户数据均在专用频段上通过PC5接口广播发送，因此短距离直连通信场景下LTE-V2X车联网系统在用户面面临着虚假信息、假冒终端、信息篡改/重放、隐私泄露等安全风险。

利用PC5无线接口的开放性，攻击者可以通过合法的终端及用户身份接入系统并且对外恶意发布虚假信息；攻击者可以利用非法终端假冒合法车联网终端身份，接入直连通信系统，并发送伪造的业务信息；攻击者可以篡改或者重放合法用户发送的业务信息，这些都将影响车联网业务的正常运行，严重危害周边车辆及行人的道路交通安全。此外，利用PC5无线接口的开放性，攻击者可以监听获取广播发送的用户标识、位置等敏感信息，进而造成用户身份、位置等隐私信息泄露。严重时，用户车辆可能被非法跟踪，直接威胁着用户的人身安全。

除了用户面数据交互，Mode 3模式下车联网终端及UE型路侧设备还需接收LTE eNB基站下发的无线资源调度指令。因此，在Mode 3模式下V2X系统同样面临着：伪基站、信令窃听、信令篡改/重放等安全风险。

2.2 业务应用

LTE-V2X业务应用包括基于云平台的业务应用以及基于PC5/V5接口的直连通信业务应用。

基于云平台的应用以蜂窝通信为基础，在流程、机制等方面与移动互联网通信模式相同，自然继承了“云、管、端”模式现有的安全风险，包括假冒用户、假冒业务服务器、非授权访问、数据安全等。在未经认证的情况下，攻击者可以假冒车联网合法用户身份接入业务服务器，获取业务服务；非法业务提供商可以假冒车联网合法业务提供商身份部署虚假业务服务器，骗取终端用户登录，获得用户信息。在未经访问控制的情况下，非法用户可以随意访问系统业务数据，调用系统业务功能，使系统面临着信息泄露及功能滥用的风险。业务数据在传输、存储、处理等过程中面临着篡改、泄露等安

全风险。

直连通信应用以网络层PC5广播通道为基础，在应用层通过V5接口实现，该场景下主要面临着假冒用户、消息篡改/伪造/重放、隐私泄露、消息风暴等安全风险。利用PC5/V5无线接口的开放性，攻击者可以假冒合法用户身份发布虚假的、伪造的业务信息，篡改、重放真实业务信息，造成业务信息失真，严重影响车联网业务安全；同时，攻击者可以在V5接口上窃听传输的业务信息，获取用户身份、位置、业务参数等敏感数据，造成用户隐私泄露；此外，攻击者还可通过大量发送垃圾信息的方式形成消息风暴，使终端处理资源耗尽，导致业务服务中断。

2.3 车载终端

车载终端承载了大量功能，除了传统的导航能力，近年来更是集成了移动办公、车辆控制、辅助驾驶等功能。功能的高度集成也使得车载终端更容易成为黑客攻击的目标，造成信息泄露，车辆失控等重大安全问题。因此车载终端面临着比传统终端更大的安全风险。

1、接口层面安全风险

车载终端可能存在多个物理访问接口，在车辆的供应链、销售运输、维修维护等环节中，攻击者可能通过暴露的物理访问接口植入有问题的硬件或升级有恶意的程序，对车载终端进行入侵和控制。

另外，车载终端通常有多个无线连接访问接口，攻击者可以通过无线接入方式对车载终端进行欺骗、入侵和控制。如通过卫星或基站定位信号、雷达信号进行欺骗，无钥匙进入系统入侵等。

2、设备层面安全风险

访问控制风险：当车载终端内、车载终端与其它车载系统间缺乏适当的访问控制和隔离措施时，会使车辆整体安全性降低。

固件逆向风险：攻击者可能通过调试口提取系统固件进行逆向分析。设备的硬件结构、调试引脚、Wi-Fi系统、串口通信、MCU（Microcontroller Unit）固件、CAN总线数据、T-BOX指纹特征等均可能被逆向分析，进而利用分析结果对终端系统进行进一步攻击。

不安全升级风险：黑客可能引导系统加载未授权代码并执行，达到篡改系统、植入后门、关闭安全功能等目的。

权限滥用风险：应用软件可能获得敏感系统资源并实施恶意行为（如GPS跟踪，后台录音等），给行车安全和用户信息保护带来了很大的安全隐患。

系统漏洞暴露风险：如果系统版本升级不及时，已知漏洞未及时修复，黑客可能通过已有的漏洞

利用代码或者工具能够对终端系统进行攻击。例如，黑客可能利用漏洞提权或关闭安全功能，发送大量伪造的数据包，对车载终端进行拒绝服务攻击。

应用软件风险：车载终端上软件很多来自外部，可能缺少良好的编码规范，存在安全漏洞。不安全的软件一旦安装到设备上，很容易被黑客控制。

数据篡改和泄露风险：关键系统服务和应用内的数据对辅助驾驶和用户对车况判断非常关键。数据被篡改可能导致导航位置错误、行车路径错误、车附属传感内容错误，车载应用的相关内容不正确。内容数据的泄露同样会造成诸多安全问题和隐患。

2.4 路侧设备

路侧设备是LTE-V2X车联网系统的核心单元，它的安全关系到车辆、行人和道路交通的整体安全。它所面临的主要安全风险如下：

1、非法接入：RSU通常通过有线接口与交通基础设施及业务云平台交互。黑客可以利用这些接口接入RSU设备，非法访问设备资源并对其进行操作和控制，从而造成覆盖区域内交通信息混乱。攻击者甚至还能通过被入侵或篡改的路侧设备发起反向攻击，入侵整个交通专用网络及应用系统，在更大范围内危害整个系统的安全。

2、运行环境风险：与车载终端类似，RSU中也会驻留和运行多种应用、提供多种服务，也会出现敏感操作和数据被篡改、被伪造和被非法调用的风险。

3、设备漏洞：路侧设备及其附件（智能交通摄像头等终端）可能存在安全漏洞，导致路侧设备被远程控制、入侵或篡改。

4、远程升级风险：通过非法的远程固件升级可以修改系统的关键代码，破坏系统的完整性。黑客可通过加载未授权的代码并执行来篡改系统、关闭安全功能，导致路侧设备被远程控制、入侵或篡改。

5、部署维护风险：路侧设备固定在部署位置后，可能由于部署人员的失误，或交通事故、风、雨等自然原因导致调试端口或通信接口暴露或者部署位置变动，降低了路侧设备物理安全防御能力，使破坏和控制成为可能。

3 LTE-V2X车联网系统安全需求

本节从网络通信、业务应用、车载终端和路侧设备三个方面讨论LTE-V2X车联网系统安全需求。

3.1 网络通信

LTE-V2X网络通信安全包含蜂窝通信接口通信安全和直连通信接口通信安全，在系统设计时应满足如下安全需求：

蜂窝通信接入过程中，终端与服务网络之间应支持双向认证，确认对方身份的合法性；

蜂窝通信过程中，终端与服务网络应对LTE网络信令支持加密、完整性以及抗重放保护，对用户数据支持加密保护，确保传输过程信息中不被窃听、伪造、篡改、重放；

直连通信过程中，系统应支持对消息来源的认证，保证消息的合法性；支持对消息的完整性及抗重放保护，确保消息在传输时不被伪造、篡改、重放；应根据需要支持对消息的机密性保护，确保消息在传输时不被窃听，防止用户敏感信息泄露；

直连通信过程中，系统应支持对真实身份标识及位置信息的隐藏，防止用户隐私泄露。

3.2 业务应用

基于云平台的业务应用与移动互联网“云、管、端”的业务交互模式相同，故其安全需求与现有网络业务应用层安全需求基本一致，需确保业务接入者及服务者身份的真实性、业务内容访问的合法性、数据存储、传输的机密性及完整性，平台操作维护管理的有效性，并做好日志审计确保可追溯性。

基于直连通信的业务应用具有新的特点，需要满足传输带宽、处理实时性等各方面要求，由此要求安全附加信息尽量精简，运算处理时间尽量压缩，以满足车联网业务快速响应的特点。在业务消息的传输过程中，系统还应：

支持数据源的认证，保证数据源头的合法性，防止假冒终端或伪造的数据信息；

应支持对消息的完整性及抗重放保护，防止消息被篡改、重放；根据需要可支持消息的机密性，保证消息在传输时不被窃听，防止用户私密信息泄露；

应支持对终端真实身份标识及位置信息的隐藏，防止用户隐私泄露。

3.3 车载终端和路侧设备

车载终端和UE型RSU具有很多共同的安全需求，其内容涉及到硬件设计、系统权限管理、运行环境安全、资源安全管理等方面，主要安全需求如下：

- 车载终端和UE型路侧设备应注意有线和无线接口的安全防护。设备应具有完备的接入用户权限管理体系，对登录用户做可信验证并且合理分配用户权限，根据不同用户权限进行不同操作处理。另外，关键芯片的型号及具体管脚功能，敏感数据的通信线路应尽量隐蔽。
- 车载终端和UE型路侧设备应具备对敏感数据的存储和运算进行隔离的能力。
- 车载终端和UE型路侧设备应支持系统启动验证功能，固件升级验证功能，程序更新和完整性验证功能以及环境自检功能，确保基础运行环境的安全。
- 车载终端和UE型路侧设备应支持访问控制和权限管理功能，确保系统接口、应用程序、数据不被越权访问和调用。
- 车载终端和UE型路侧设备应具有安全信息采集能力和基于云端的安全管理能力。设备可通过安全信息采集与分析发现漏洞与潜在威胁，同时上报云端，由云端平台修补相应漏洞，并通知其他终端防止威胁扩散。
- 车载终端和UE型路侧设备应具有入侵检测和防御能力。设备可通过分析车内应用的特点制定检测和防御规则，检测和隔离恶意消息。对于可能的恶意消息，可进一步上报给云端平台进行分析和处理。

除了上述共同的安全需求外，UE型RSU还应支持物理安全防护能力、防拆卸或拆卸报警能力、部署位置变动的报警能力等。eNB型RSU形态与eNB类似，应参考现有eNB设备安全技术要求及安全防护要求进行安全保护。

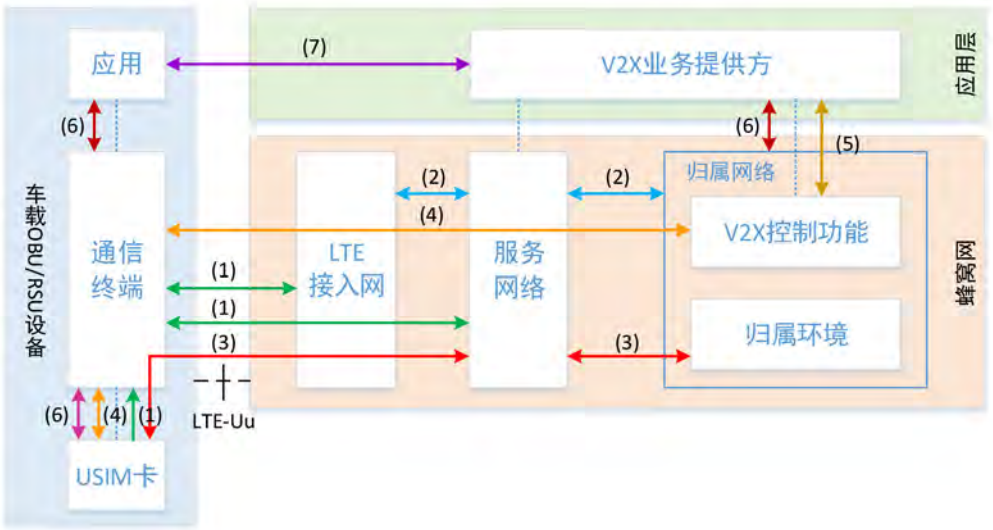
4 LTE-V2X车联网系统安全架构及机制

本节介绍蜂窝通信场景和直连通信场景下LTE-V2X车联网系统安全架构，随后介绍各部分的安全机制。

4.1 系统安全架构

4.1.1 蜂窝通信场景系统安全架构

为了支持基于LTE-Uu接口的车联网业务需求，3GPP标准组织参照邻近通信业务的系统方案在现有LTE网络的基础之上引入了V2X控制功能网元，对车联网终端及业务进行管控，并对上层业务提供方提供服务支撑，满足业务需要。在此网络架构下，LTE-V2X车联网系统安全架构如图4-1所示。为了清晰，此处以车载终端为例表示终端设备，除此之外它还可以是UE型RSU或者行人便携终端。



注：漫游场景下，V2X控制功能可作为Proxy位于服务网络。

图4-1 LTE-V2X蜂窝通信场景系统安全架构示意图

蜂窝通信场景下，LTE-V2X车联网系统安全架构包含如下八个安全域：

1、网络接入安全：车联网终端接入到LTE网络的信令及数据安全，如（1）所示，包括接入层安全和非接入层安全。

2、网络域安全：LTE系统网元之间信令及数据交互的安全，如（2）所示，包括LTE接入网与服务网络之间，服务网络与归属网络之间的安全交互。

3、认证及密钥管理：车联网终端与LTE网络的接入认证以及密钥管理，如（3）所示。

4、车联业务接入安全：车联网终端与V2X控制功能之间的安全，如（4）所示。

5、车联业务能力开放安全：V2X控制功能与LTE-V2X业务提供方之间的安全，如（5）所示。

6、网络安全能力开放：LTE系统向应用层开放网络层安全能力，提供双向身份认证及密钥协商服务，如（6）所示。

7、应用层安全：车联网终端应用和LTE-V2X业务提供方之间在应用层提供的数据通信安全和用户隐私安全，如（7）所示。

4.1.2　直连通信场景系统安全架构

直连通信场景下LTE-V2X车联网系统安全架构如图4-2所示。其中RSU设备可以通过有线接口与交通信号控制系统及业务云平台交互。

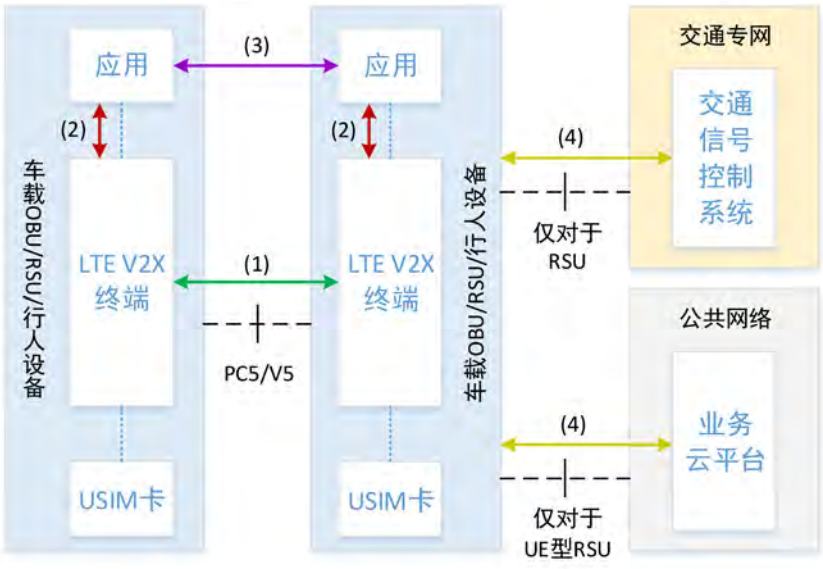


图4-2　LTE-V2X直连通信场景系统安全架构示意图

直连通信场景下，LTE-V2X车联网系统安全架构包含如下四个安全域：

1、网络层安全：车联网终端在网络层提供的数据通信安全和用户隐私安全，如（1）所示。

2、安全能力支撑：网络层向应用层提供的安全能力支撑，保护用户隐私信息，如（2）所示。

3、应用层安全：车联网终端在应用层提供的数据通信安全和用户隐私安全，如（3）所示。

4、外部网络域安全：RSU设备与其他网络域设备之间的接入及数据交互安全，如（4）所示，是LTE-V2X车联网与其他系统之间的安全边界。

4.2 网络层安全机制

4.2.1 蜂窝通信场景

对应于图4-1，LTE-V2X车联网系统在网络层包含安全域（1）至（6），负责网络接入、数据传输的安全以及对外的安全能力开放。目前所采取的安全机制如下。

1、网络接入安全：继承LTE网络现有安全机制，采用接入层（AS）和非接入层（NAS）两层安全体系保障传输安全。接入层安全负责终端与LTE基站（eNB）之间的安全，包括对AS层控制面信令的机密性和完整性安全保护，以及对用户面数据的机密性安全保护。非接入层安全负责车联网终端与LTE核心网移动性管理实体（MME）之间的安全，包括NAS层控制面信令的机密性和完整性安全保护。

2、网络域安全：继承LTE网络现有安全机制，将网络划分为不同的安全域，使用NDS/IP的方式（IKE+IPsec）保护网络域的安全，在网元之间提供双向身份认证、机密性、完整性和抗重放保护。它使用NDS/AF定义的机制实现证书管理。

3、认证及密钥管理：继承LTE网络现有安全机制，在终端与LTE核心网间基于运营商安全凭据（如根密钥K）实现EPS-AKA双向认证，保证终端和网络身份的合法性。同时，基于LTE分层密钥架构体系，生成AS层及NAS层会话密钥，保证AS层和NAS层的数据传输安全。终端及核心网从密钥K衍生出中间密钥Kasme，再由中间密钥Kasme衍生出AS层和NAS层的完整性保护密钥和加密密钥，用于对信令和数据的完整性保护和加密。

4、车联业务接入安全：车联网系统新增的安全域，对于LTE核心网而言属于应用层安全。它在终端与其归属网络的V2X控制功能之间提供双向认证，对终端身份提供机密性保护；在终端与V2X控制功能之间对配置数据提供传输时的完整性保护、机密性保护和抗重放保护。它包括UICC配置传输安全和终端数据传输安全。

UICC配置传输安全的基本机制如下。终端部署应用后，UICC上保存的配置参数可能需要更新以反映系统配置的更改。这时可采用UICC OTA机制对更新的配置数据进行传输保护。

终端数据传输安全根据消息发起方的不同在机制流程上有所区别。对于终端发起的消息，可通过GBA（Generic Bootstrapping Architecture）机制在终端与V2X控制功能之间进行双向认证并协商会话密钥，以此为基础建立PSK TLS安全连接。对于网络侧发起的消息，需根据不同情况进行不同处理。如果终端与V2X控制功能之间在先前消息交互时建立的PSK TLS安全连接仍然存在，则使用已有的PSK TLS会话完成消息的安全传输；否则，需使用GBA Push机制在终端与V2X控制功能之间进行双向认证并协商会话密钥，以此为基础重新建立PSK TLS安全连接。

5、车联业务能力开放安全：车联网系统新增的安全域，保证对上层应用提供LTE-V2X业务能力开放过程中的接入及数据传输安全。它可采取类似于网络域安全的方法来保护，在不同安全域之间采用IPSec、TLS等安全机制为业务提供双向认证、加密、完整性保护和抗重放的安全保障。

6、网络安全能力开放：继承LTE网络现有GBA、GBA Push等安全机制，利用LTE网络在终端侧USIM卡以及核心网中已有的密钥信息对终端进行身份认证并且为应用层协商会话密钥。LTE-V2X业务提供方可利用网络层开放的安全能力在应用层建立安全的通信通道，保证业务数据传输的安全，降低对于应用层安全机制的依赖。

4.2.2 直连通信场景

对应于图4-2，LTE-V2X车联网系统在网络层包含安全域（1）、（2）和（4），负责基于PC5接口数据传输的安全以及对上层应用的安全能力支撑。目前所采取安全机制如下。

1、网络层安全：根据3GPP组织的定义，终端在网络层不采取任何机制对PC5接口上广播发送的直连通信数据进行安全保护，数据的传输安全完全在应用层V5接口保障。网络层仅提供标识更新机制对用户隐私进行保护。终端通过随机动态改变源端用户层二标识和源IP地址，防止用户身份标识信息在PC5广播通信的过程中遭到泄露，被攻击者跟踪。

2、安全能力支撑：网络层向应用层提供安全能力支撑，采取用户标识跨层同步机制确保源端用户层二标识、源IP地址与应用层标识同步更新，防止由于网络层与应用层用户身份标识更新的不同步，导致用户标识关联信息被攻击者获取，用户隐私信息遭到泄露。

3、外部网络域安全：采取类似于网络域安全的方法来保护。在RSU设备与其他网络域设备之间通过物理隔离防护的方法保证传输链路的物理安全，或者通过建立IPSec、TLS等安全通信通道的方法，为跨网络域数据及信息交互提供双向认证、加密、完整性保护和抗重放的安全保障。

4.3 应用层安全机制

LTE-V2X车联网业务应用安全包含基于云平台的和基于直连通信的两个部分。

基于云平台的LTE-V2X车联网业务应用与传统移动互联网应用类似，可采取现有安全机制在软硬件、系统等方面做好防护，同时可将应用层安全机制（如图4-1（7）所示）作为蜂窝通信场景的附加安全解决方案，确保业务数据传输时的安全，这里不再赘述。本节主要关注直连通信场景下应用层（如图4-2（3）所示）的安全机制。

4.3.1 直连通信安全

为了实现OBU、RSU等V2X设备间的安全认证和安全通信，LTE-V2X车联网系统使用基于公钥证书的PKI机制确保设备间的安全认证和安全通信，采用数字签名等技术手段实现V2V/V2I/V2P直连通信安全。密码算法应采用国家密码管理局批准的国密算法，数字证书应符合国家标准或者行业标准的技术要求。

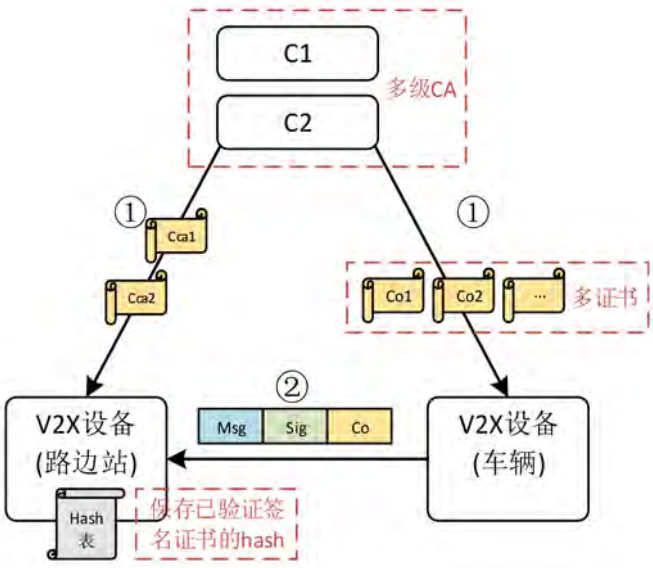


图4-3 安全的直连通信流程

图4-3以V2I通信为例给出了典型的V5接口安全通信过程，具体如下：

1、CA证书管理系统以安全的方式向OBU终端颁发公钥证书（安全消息证书Co1、Co2、…）用于签发PC5/V5直连通信消息，向RSU下发CA公钥证书（Cca1、Cca2）用于验证OBU公钥证书真实性

的。为了保护用户隐私，CA管理系统可以一次下发多个采用假名方式标识的公钥证书供OBU终端随机使用。

2、OBU终端使用公钥证书（Co）对应的私钥对业务消息内容进行数字签名，之后将业务消息内容、消息签名值以及所使用的的公钥证书/证书链组建成完整PC5/V5直连通信消息在空口上广播发送。

3、接收到PC5/V5直连通信消息后，RSU使用CA公钥证书（Cca1、Cca2）验证消息中携带的OBU公钥证书或证书链，然后利用OBU公钥证书里的公钥验证消息签名，以检查消息的完整性。

4、成功验证OBU公钥证书（Co）后，RSU可将该证书的Hash值保存在本地，后续可通过Hash值验证该证书，从而减少证书验证所需的密码运算开销。

4.3.2　CA基础设施构建

为了能够对基于数字证书的应用层安全机制提供有效支撑，LTE-V2X车联网系统需要建立一套完整的CA管理系统，实现证书颁发、证书撤销、终端安全信息收集、数据管理、异常分析等一系列与安全相关的功能，确保V2X业务的安全。

4.3.2.1　系统框架

CA管理系统需要管理车载终端设备、路侧设备以及包括制造工厂、注册机构、授权机构和服务机构在内的与LTE-V2X车联网业务相关的各个部门，其总体框架图如图4-4所示。

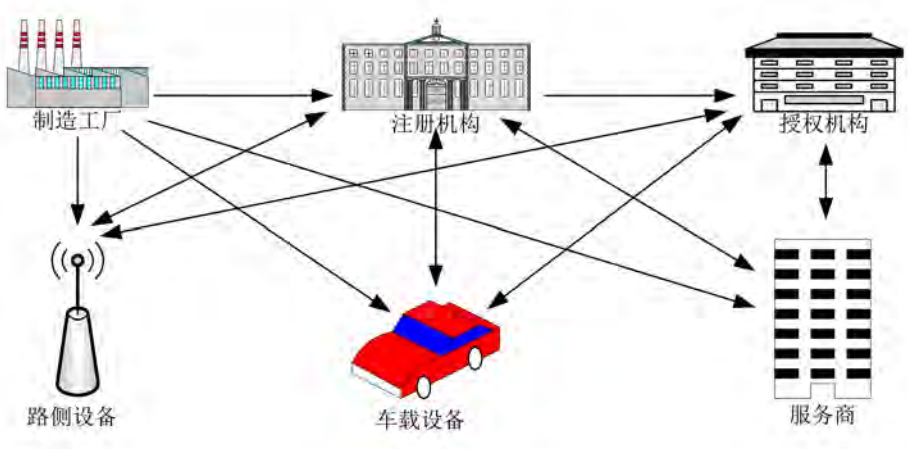


图4-4　LTE-V2X安全基础设施总体框架

制造工厂负责LTE-V2X车联网系统相关设备的生产，如车载终端设备、路侧设备、后台系统所使用的安全设备等。

注册机构负责车载设备及路侧设备的认证，只有经过相关注册机构的认证，这些设备才能在系统中使用。LTE-V2X车联网系统中注册机构为颁发注册证书的CA。

授权机构负责车载设备及路侧设备的授权，只有经过相关授权机构的授权，这些设备才能在系统中播发或接收授权许可的消息。LTE-V2X车联网系统中授权机构为颁发安全消息证书的安全消息CA和颁发服务消息证书的服务消息CA。

根据LTE-V2X车联网业务管理模式的不同，注册机构和授权机构可以是同一个管理部门负责，也可以由不同的管理部门负责。

4.3.2.2 基本工作流程

LTE-V2X车联网CA管理系统的基本工作流程为：

1、注册机构对LTE-V2X车联网设备和服务机构的资格进行认证，并向通过认证的实体颁发注册（认证）证书；

2、LTE-V2X车联网设备利用注册证书向授权机构申请LTE-V2X车联网系统的功能授权；

3、授权机构根据LTE-V2X车联网设备的认证证书向其颁发授权证书，授权证书中描述了该设备所能执行的功能和安全操作；

4、LTE-V2X车联网设备利用授权证书及其对应的公私钥对收发的消息进行签名、验签或加解密等安全操作。

4.3.2.3 各环节职责

1、制造厂商

制造厂商负责LTE-V2X车联网系统相关设备的生产，如车载终端、路侧设备、后台系统所使用的安全设备等。在生产过程中，设备的唯一标识将被写入，该标识在设备的整个生命周期内是不再改变。在安全的生产环境下，原始的设备认证和授权机制被写入设备，后续可以通过该认证和授权机制将缺省的授信注册机构和授信授权机构信息写入设备。

在设备的生产过程中，以下数据将在安全的环境下写入设备：

- 设备的唯一标识；
- 缺省颁发的注册公钥证书，通过这些公钥证书，设备可以开始一个注册过程；

- 缺省颁发的授权公钥证书，通过这些公钥证书，设备可以同其他设备进行通信；
- 颁发的证书及其证书链（可选）。

设备生产过程中也可以设备支持的USIM为信任根，基于LTE网络GBA安全机制实现设备的初始配置，以降低初始配置过程对制造厂商安全生产环境的依赖。此时，需要写入设备的原始信息将简化为：

- 设备唯一标识；
- 授信注册机构的服务域名或地址信息。

注册公钥证书、授权公钥证书等信息可以以安全方式在线申请下载。

2、注册机构

注册机构负责LTE-V2X车联网设备的认证，相关设备只有经过注册机构的认证才能在系统中使用。注册机构首先验证LTE-V2X车联网设备是否合法，然后为合法的设备颁发认证证书，即注册证书。认证证书用于申请终端授权证书。

注册证书的主要内容为：

- 权限许可描述，用以限定可被授予的最大权限；
- 应用区域描述，用以限定可被授予的最大应用地理区域。

注册机构的主要应用特点是：

- 车联网设备可以注册到多个不同的注册机构；
- 允许多级注册机构体系，高级注册机构可授权低级注册机构为车联网设备颁发证书；
- 注册机构可要求车联网设备定期进行重注册。

3、授权机构

授权机构负责LTE-V2X车联网设备的授权，只有经过相关授权机构的授权，LTE-V2X车联网设备才能在系统中播发或接收授权许可的消息。授权机构首先验证颁发给设备的认证证书的有效性，然后为合法的设备颁发授权证书，即安全消息证书或服务消息证书。

授权证书的主要内容为：

- 权限许可描述，以限定设备可发送的安全消息类别；
- 权限及优先级描述，以限定设备可发送的服务消息类别及其优先级；
- 应用区域描述，以限定该设备的应用地理区域。

授权机构的主要应用特点是：

- 可接收来自多个注册机构的注册证书，此时证书的适用范围为各证书许可的交集；
- 允许多级授权机构体系，高级授权机构可授权低级授权机构为车联网设备颁发证书；
- 车联网设备可注册至多个不同的授权机构；
- 授权机构可要求车联网设备定期进行重授权。

4.3.3　可能的部署方案

LTE-V2X车联网安全基础设施是LTE-V2X安全通信的重要组成部分，它的部署模式与车联网业务及其管理模式紧密相关。这里以车辆主动安全业务为例，简要介绍车联网应用于道路安全场景时可能的CA部署方案。

4.3.3.1　集中式部署方案

为了实现车辆主动安全业务并保护用户隐私，LTE-V2X车联网系统需要使用由注册CA、V2V假名CA、V2I授权CA和证书撤销CA等构成的PKI体系。

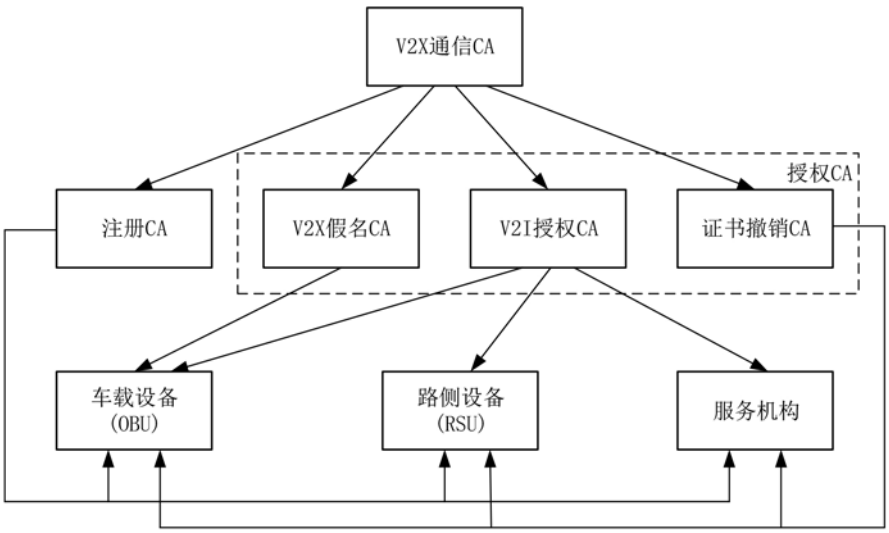


图4-5　集中式安全基础设施部署方式

图4-5给出了一种可能的CA部署方案，其采用了单一根CA的方式，各部分功能如下。

- V2X通信CA：LTE-V2X通信安全的根CA，是LTE-V2X车联网通信PKI体系的安全锚点。此CA可向其他V2X安全通信子CA颁发证书，从而构建LTE-V2X车联网安全通信CA系统和证书体系。

• 注册CA：负责向符合入网条件的车载终端、路侧设备和服务机构等实体颁发注册证书。这些实体使用注册证书进一步向其他授权CA申请实现某种安全通信能力的证书。例如向V2V假名CA申请用于车-车匿名通信的假名证书，向V2I授权CA申请用于车-路通信的V2I通信证书。

• V2X假名CA：负责向车载终端颁发用于车-车匿名通信的假名证书。该证书用于签发车辆基本安全信息（Basic Safety Message，BSM），实现对用户车辆标识的匿名保护。

• V2I授权CA：负责向车载终端、路侧设备和服务机构颁发用于车辆与路侧设备进行安全通信的证书。例如与红绿灯等交通基础设施相连的路侧设备使用该证书对其播发的消息进行签名，或者警车等特种车辆对其播发的消息进行签名。

• 证书撤销CA：负责签发各种证书的证书撤销列表。

集中式部署方案需要部署统一的CA体系结构，所有的子CA都在同一个根CA下管理。根CA可由车联网管理责任部门负责运营维护。这种部署方式适用于对LTE-V2X车联网有明确主管责任部门进行统一管理的场景。集中式部署的优点是所有的证书由统一的根CA管理，管理比较简单，缺点是不能重用现有的CA系统，需要重新建立新的CA体系。

4.3.3.1 分布式部署方案

针对车辆主动安全业务，图4-6给出了另一种可能的CA部署方案，其通过CA之间的交叉认证实现可信的PKI体系。

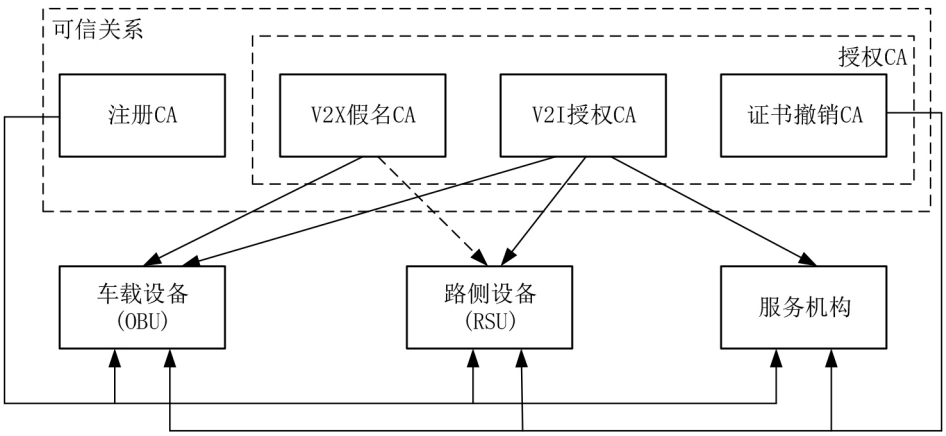


图4-6 分布式安全基础设施部署方式

分布式部署方案不需要有共同的根CA，不同的业务可以设置不同的根CA，但需要在不同的根CA之间建立互信关系。这种部署方式适用于多部门共同对LTE-V2X车联网进行管理和维护的场景。这种方式的优点是容易对接现有的管理机制，可在现有CA系统中增加相应的功能即可，缺点是需要执行交叉认证，增加了消息长度和消息处理时延。

4.4 终端和路侧设备安全机制

车载终端和路侧设备安全是LTE-V2X车联网安全的关键环节。对车载终端的攻击轻则可能导致车辆故障或者被盗，致使用户财产受损，重则可能导致车毁人亡的重大交通事故。对路侧设备的攻击会对车联网系统整体造成影响，严重时可能造成交通系统混乱。

针对车载终端和UE型路侧设备的共同点，可以从接口层面和设备层面两个方面保证其安全性。

1、接口层面安全机制

车载终端和UE型路侧设备的关键芯片要尽量采用无管脚暴露的封装形式，商用产品要禁用调试接口。

车载终端和UE型路侧设备需要进行访问控制，检查访问者是否具备合法的令牌、口令或证书，提升攻击的难度。同时进一步设置合适和统一的安全策略，如访问密码复杂度，对关键资源访问采用双重认证等，进一步提升防御非法攻击者获取访问入口的能力。

除此之外，RSU设备存在与其他网络域设备的外部接口，如图4-2（4）所示。这些接口是RSU设备与交通信号控制系统、业务云平台之间交互的通道，是车联网与其他系统间的安全边界。为了防止网络跨安全域的攻击，可以在接口上采取IPSec、TLS等安全措施实现双向认证、数据机密性、完整性及防重放保护。

2、设备层面安全机制

系统隔离机制：以芯片/硬件/固件安全为基础，采用硬件隔离和安全域隔离的方式将具有高安全要求特征的核心驾驶系统和驾驶辅助应用与具有低安全要求特征的车载娱乐系统和娱乐应用进行隔离，以保护敏感数据和操作。例如仅在SPU（Secure Processing Unit，安全处理器）/TEE（Trusted Execution Environment，可信执行环境）/SE（Secure Element，安全单元）中进行密码运算及敏感操作。

安全启动和安全升级机制：采用对软件包进行数字签名的技术，通过校验系统和应用软件的数字签名确定软件包是否合法，从而保证系统只能引导合法的系统和应用。

安全存储和传输机制：为上层应用提供基于软件或硬件的加解密服务，保护敏感数据。提供加密和签名服务，保证发送消息的机密性和完整性。

另外，UE型与eNB型路侧设备还需要具备保证部署环境安全的机制，例如对位置和工作状态进行监控，预警部署环境威胁，对设备外壳进行防拆解改造，通过防拆解电路报警机制加强抵御物理攻击的能力。eNB型RSU还应结合现有eNB设备安全技术机制及安全防护机制进行安全保护。

4.5 安全运营和管理

车联网系统涉及到的处理、管控环节众多，虽然可以在网络、应用、终端、数据、车辆等各方面采取主动安全机制预防来自各方的攻击，然而，不可避免地仍会存在潜在的安全漏洞，安全事件也仍会发生。为了进一步提高车联网系统发现和应对安全事件的能力，车联网还应加强安全运营及管控，提高系统的安全防御能力。

车联网安全运营及管理体系是一套完整的系统安全解决方案，基本结构如图4-7所示。它从采集、检测、发现、评估、调查和响应等环节对车联网安全事件进行全生命周期的监测和管理。车联网安全运营管理体系能够收集和存储来自每个节点的安全事件和安全问题，并且通过对安全事件的高级分析，关联解析出单个节点无法分析出的安全威胁，提升安全威胁事件预警的准确率，并以可视化的方式呈现，从而综合提升LTE-V2X车联网安全的管控能力。

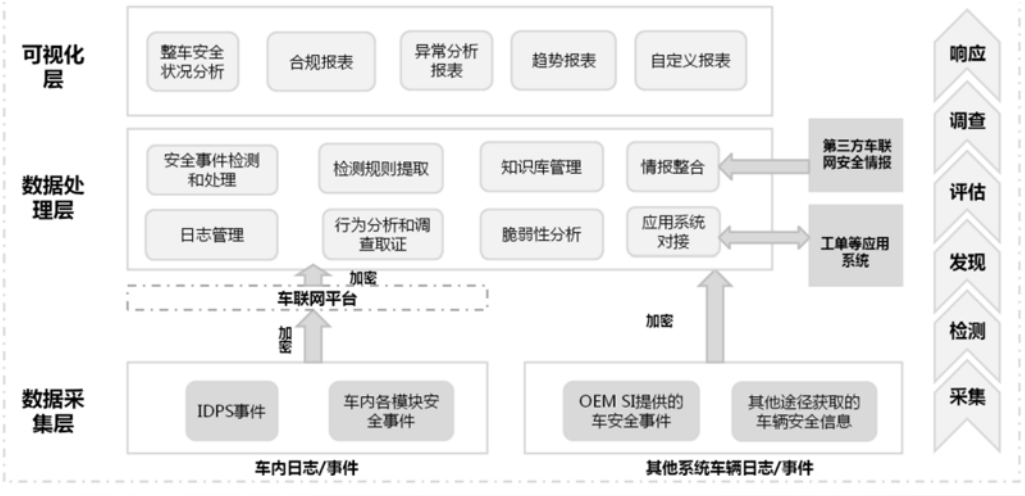


图4-7 车联网安全运营及管理体系

车联网安全运营及管理体系包含如下三个层次：

1、数据采集层

数据采集层主要负责车联网安全事件及V2X应用异常行为的采集。该层收集各类安全事件，包括 ：入侵检测和防御（IDPS）事件、车内各模块的安全事件、OEM和需提供集成商（OEM&SI）提供的安全事件和其他途径获取的安全事件，并上报到安全运营管理平台。该平台将收集和存储上报的大量信息安全相关信息。

2、数据处理层

数据处理层主要负责车联网安全事件的分析和处理。除了从数据采集层收集信息外，该层还会从第三方收集车联网安全情报，然后进行分析、去重，并结合历史威胁以及威胁情报，降低事件的误报率，通过安全事件处理机制，派发工单，对安全事件进行处理。

3、可视化层

可视化层主要负责车联网威胁和风险的可视化呈现，这部分给运营人员呈现一个威胁可读、可视、可感知的平台，对历史安全事件进行留存，便于事件调查、分析和取证。

5 总结和展望

LTE-V2X是C-V2X车联网采用的主流技术方案，由于它能够更好的发挥现有移动蜂窝网的优势，提供更广范围的业务服务，倍受全球电信运营商、汽车企业的关注。面对车联网业务新的系统组成、新的通信场景，基于LTE的V2X车联网系统在网络通信、业务应用、车载终端、路侧设备等各个方面采取有效的安全机制，保证车联网业务数据的通信安全和用户隐私信息的安全。

为了能够有效支撑基于PKI公钥体系的应用层安全认证和安全通信机制，LTE-V2X需要建立一套完整的证书管理系统。然而，CA的部署与车联网业务管理模式紧密相关，在管理模式尚未清晰的情况下很难给出确切的部署方案建议，因此需要在对车联网证书管理系统已有认知的基础上，推动行业及相关主管部门加快这方面的讨论，以便形成适合我国的部署方案。

车联网安全应以满足汽车生产及应用为首要目标，下一步应与汽车生产企业紧密合作，注重来自于车厂的产业需求，寻求高效、便捷的安全技术方案。同时，参与各方应做好沟通衔接，搭建测试平台，分阶段推进技术方案测试验证及优化，为安全技术方案落地提供测试依据。

随着蜂窝通信技术的不断发展，LTE-V2X车联网也将朝向5G-V2X技术方向演进。基于5G新空口及网络切片技术，低时延、高可靠通信将被支持，用于实现自动驾驶等更加丰富的车联网业务应用。与此同时，LTE-V2X车联网还将与移动边缘计算技术相结合，形成分层、多级边缘计算体系，满足高速、低时延车联网业务处理及响应的需要。这些新的技术演进及发展都将给车联网安全体系带来全新的影响。为了进一步提高新系统的运行效率，降低安全信息带宽占用及密码运算开销，可以进一步探讨轻量级安全、物理层安全等新技术在演进系统中应用的可行性，这些都是下一阶段C-V2X车联网安全技术研究可关注的方向。

6 主要贡献单位


中国移动
China Mobile


大唐电信科技产业集团


CAICT 中国信通院


HUAWEI


ZTE中兴


中国一汽


VOLVO


TOYOTA
INFOTECH
Envisioning Mobility


Qualcomm


Neusoft


重庆邮电大学


中国电信
CHINA TELECOM
世界触手可及


360
www.360.cn


NAVINFO
四维图新


Continental


延锋伟世通
Yanfeng Visteon


Genvict金溢


千方科技
CHINA TRANSINFO


SAMSUNG


信长城

IMT-2020

联系方式
电话：+86-10-62300164
邮箱：imt2020@catr.cn